STATEMENT OF NEED

1. Automated system for the processing of specimens for cytological examination

The contractor shall provide the James A Haley Veterans' Hospital, Pathology and Laboratory Medicine Service, the Hologic ThinPrep system or an equivalent state-of the art, FDA approved, automated cytology processing system(s) that will provide a mono-layer of cellular material using liquid based technology. Contractor shall supply all instrumentation, collection vials, reagents, filters, slides, and all disposables and consumables required for specimen processing.

2. Total tests per year are estimated at 2000 GYN and 5500 Non-GYN specimens per year.

3. Reagent Rental / Cost per Test Award

The contract price includes costs covering (a) equipment use (reagent rental), (b) all necessary filters, supplies and reagents (c) maintenance and repair to keep the equipment in good operating condition (d) operational hardware and software upgrades (e) user training for government personnel (f) operator's and service manuals (also available in electronic format) (g) preventive maintenance per manufacturer's recommendations (h) complete service support, and (i) reagents' delivery cost. Contractor is required to provide delivery and installation of equipment at no additional charge, and return shipping costs at end of contract.

4. Required Characteristics for automated cytology processing system:

a. An automated processing system(s) capable of processing up to 50 GYN and non-GYN lung, bladder, gastrointestinal, fine needle aspirates, etc., specimens per day. The system must be able to run one sample at a time without reagent or consumable wastage.

b. System shall produce mono-layer slides with a thin, even layer of diagnostic cellular material.

c. System shall maximize the recovery of diagnostic cells while removing blood, mucus, non-diagnostic debris, and other artifacts that impede diagnostic analysis without adversely affecting the appearance of cells.

d. All models shall perform satisfactorily at any laboratory temperature between 59 and 86 degrees F (15 and 30 degrees Celsius). All models shall perform satisfactorily at any laboratory relative humidity between 10 and 70%.

e. Physicals characteristics include NTE 200 lbs, and a footprint no greater than 6 ft. by 3 ft. Electrical characteristics 120 VAC plus or minus 10%, 8 amps, 60 Hz.

g. Sample medium must remain stable at room temperature for up to 90 days and be FDA approved to be used for HPV testing concurrently. Specimen prep between collection and loading processor should be minimal.

h. Any special items required for maintaining the equipment in optimal condition, such as but not limited to UPS, surge suppressors, etc., will be the responsibility of the vendor. Any maintenance, time and materials needed to keep the special items in working order

will be the responsibility of the vendor.

5. Training and Maintenance

a. Vendor will provide off-site training for one cytotechnologist and one cytology prep technician at no cost to the VA. Vendor will provide on-site educational offerings including slide sets to enhance the competence of the cytotechnologists.

b. Preventive Maintenance shall be performed per manufacturer's guidelines.

c. Instrument service to be provided weekdays, 8-5pm. Expected response to service call time from initial call to vendor to service engineer arriving on site should be no more than 24 hours. A 24/7 Technical Support Hotline must be available for in-house troubleshooting.

With No Sensitive Data but Requires Training

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

VA INFORMATION CUSTODIAL LANGUAGE:

a. Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

b. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

c. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

d. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

SECURITY INCIDENT INVESTIGATION:

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

LIQUIDATED DAMAGES FOR DATA BREACH:

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

SECURITY CONTROLS COMPLIANCE TESTING :

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

TRAINING:

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete VA Privacy and Information Security Awareness and Rules of Behavior Training before being granted access to VA information and its systems.

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Rules of Behavior* before being granted access to VA information and its systems.

b. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

The Certification and Accreditation (C&A) requirements do not apply and a Security Accreditation Package is not required for this SOW.

Records Management Contract Language

The following standard items relate to records generated in executing the contract and should be included in a typical Electronic Information Systems (EIS) procurement contract:

1. Citations to pertinent laws, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.

2. Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

3. Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.

4. Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.

5. Contractor shall not create or maintain any records containing any Government Agency records that are not specifically tied to or authorized by the contract.

6. The Government Agency owns the rights to all data/records produced as part of this contract.

7. The Government Agency owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

8. Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.].

9. No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

10. Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Compliance & Business Integrity (CBI) Language for Contracts

The _____ has a CBI Program. If the contractor detects and/or suspects any noncompliance relative to the revenue cycle when providing treatment to our veterans, he/she is to notify the Contracting Officer's Representative (COR) or the _____ CBI Officer. CBI Awareness training is available on the Talent Management System website. Any contract staff who does VA work is required to take basic compliance awareness training, annual CBI refresher training. Job-specific training may be required for staff in specific positions that relates to the revenue cycle. Contact the _____ CBI Officer or COR for examples of CBI training that

would satisfy this requirement. The contractor is to show proof of completing this

training by submitting a completed copy of the VISN 6 CBI Certification Form to the

COR. You may contact the _____ CBI Officer for more information regarding CBI

training.

Rev. 9/2/13

All Contractor, Pharmaceutical Company Representative (PCR), and Healthcare Industry Representatives (HIR) will coordinate with Contracting Officer Representative for instructions so they are in compliance with James A. Haley Veterans' Hospital policies:

HPM NO. 90-25; JANUARY 2014; HEALTHCARE VENDOR ACCESS AND COMPETENCY

HPM NO. 132-04; DECEMBER 2012; SECURITY MANAGEMENT PROGRAM
HPM NO. 132-05; DECEMBER 2012; HOSPITAL IDENTIFICATION PROGRAM

HPM NO. 11-91; MAY 2013; PHARMACEUTICAL COMPANY REPRESENTATIVES

HIR are required to report to MSDU (Room GC-003), immediately after entering the facility. HIR will be required to sign into the monitoring system and print a badge for proper identification. . The Healthcare Industry Representatives for Nutrition and Food Services, Office of Information and Technology, and Social Work Services are in included in this policy; vendors (HIR) for Pharmacy Services are to follow (HPM 11-91) policy. HIR must be sponsored by a physician, a Service Chief, or their designee, for a specified date and a specified case. HIR are not permitted in patient care areas or clinics unless a prior appointment has been made.

Pharmaceutical Company Representative (PCR) refers to anyone acting on behalf of a pharmaceutical company or its business partners for the purpose of promoting the use of items managed under the VA formulary process. These items primarily include drugs, but to a lesser extent also include any medical supplies, nutritional supplements, and similar commodities managed under the VA formulary process.

a. Sign-In: PCRs may visit VA Medical care facilities no earlier than 8:00 a.m. and stay no later than 3:30 p.m., Monday through Friday, unless they receive prior approval from both the Chief of the Service that they will be visiting and the Chief of Pharmacy. Representatives visiting the JAHVH must sign in at the Pharmacy Administrative Office (Located in Trailer 78) and wear a visitor's badge as well as their company's personal name badge while in the hospital.

Vendors: Reference Hospital Memorandum Policy Number 90-25 Healthcare Vendor Access and Competency.

Contractors and/or project managers: Will be issued a PIV/ID badge in accordance with the facility PIV Policy. Contactors will contact their assigned VA Contracting Officer Representative (COR) for coordination.

Contract Personnel/Sub-Contractors: Contractors are responsible for the daily accountability and identification of all personnel assigned to their respective contract including sub-contractors. Contractors will identify personnel using the following procedures as appropriate.

Construction Project contract personnel will report to the contractor for issuance of a temporary self-adhesive identification badge. This badge will be issued on a daily basis and must include the following information: Company name, project number, date and name of individual. Contractor will maintain a daily log of all personnel.

Contract personnel not involved in an actual construction project will report to police dispatch for issuance of a numbered badge. A driver's license or photo ID will be required each day upon entering the facility, in exchange for the badge, and will be given back once the badge is returned to police dispatch. The contractor will provide Police Service with a list of names for all sub-contract personnel requiring access to the facility. It is the responsibility of the contractor to update the list as necessary.

NPR OPC; CBOCs and Off-site Lease facilities with VA Police staffing: As above with check-in with VA Police.

Off-site Lease facilities w/o VA Police staffing: Coordinate with COR, Administrative Officer, or Service Point of Contact.